System Architectural Design Description

(SADD)

NAV3i Platform Family

NAV3i Operating System

Document Control

Author:	**Jochen Becher**
Document No.:	**0000039008**
Revision No.:	**E.1**
Project:	**0000012124, SPC3.1**
Project Lead:	**Alexander Schöbel / Björn Lampart**

Change Records

Rev. No.	Comment	Date	Author
A	Initial Version	2014-09-02	A. Schöbel
	Updated all open items with exception of risk control and SOUPs	2015-01-22	J. Becher
	Updated references to SOUPs	2015-02-10	J. Becher
	Reference 3 DIOTVs instead of one large one Started to fill some risk control references but risk control table is not finished yet.	2015-02-18	J. Becher
	Added Shutdown Manager Included Review findings	2015-02-24	A. Schöbel
B	Updated document references to Application Manager 5.0 Updated version of SOUP_NVIDIA	2015-03-06	J. Becher
	Rename “Microscope Kit” to “Microscope Script” (to prevent confusion with saleable part “Microscope Kit” incl. cables, adapters…) Update graphic on page 13	2015-04-28	A. Mayer
	Renamed system to NAV3i Platform Family and subsystem to NAV3i Operating System. Updated title page. Updated table of Definitions, Acronyms and Abbreviations Minor updates to diagrams improving software and hardware decomposition Fixed some color codes in diagrams Added references to risks in rationales of safety classification Updated risk control table Improved documentation of design decisions Removed references to Exceed which is no longer part of the NAV3i Operating System installation Updated SOUP table	2015-05-08	J. Becher
	Fixed layout of foot-bar Removed unused document references Fixed inconsistencies in rationales of safety classification	2015-05-20	J. Becher
	Update for consistent naming of RFID license cards Removal of unused SOUP_RFID2. Fixed version of SOUP_UPSMAN	2015-05-21	J. Becher
C	Fixed reference to SOUP_NVIDIA document Added version of SFB Driver	2015-07-30	J. Becher
D	Introduced new software component “OS Scripts”	2015-08-19	J. Becher
E	CR2991 – IO-Tablet Gen2: Chapter 1.4: Added reference to Elatec RFID driver Chapter 3.2.1.2, SW4: added Elatec RFID driver as reference Chapter 6: Added Elatec RFID driver to SOUP list	2016-03-23	A. Schöbel

Table of Contents

1 Introduction

1.1 Purpose

This document describes the overall architectural design of the system NAV3i Platform Family / NAV3i Operating System. It depicts from a high level perspective the system's context and its static as well as dynamic structure. Where details go beyond the scope of this document the reader is referred to lower level architecture and design documents.

The intended audience for this document is development, regulatory affairs and quality assurance.

1.2 Scope

The NAV3i Platform Family / NAV3i Operating System is the common software platform for Stryker Navigation Applications. It is based on a pre-configured Windows operating system and includes a number of additional 3rd party components (SOUP, software of unknown provenance) and a number of software components developed by Stryker Navigation.

All functional requirements for the NAV3i Operating System software are provided by [DS_OS].

1.3 Definitions, Acronyms and Abbreviations

Term	Definition
API	Application Programmer's Interface
AXEDA	Marketing name of products from company PTC providing remote access to computer and different cloud services.
BIOS	**B**asic **I**nput **O**utput **S**ystem, firmware part of a computer system
CAN bus	A **C**ontroller **A**rea **N**etwork is a bus standard
CanUSB	An implementation of the CAN bus via USB.
C-Arm	Main component of an x-ray image intensifier.
CD	**C**ompact **D**isc is a digital optical disc data storage format on physical media.
CPU	**C**entral **P**rocessing **U**nit, the main processor of a computer system
CT	X-ray **C**omputed **T**omography
DICOM	**D**igital **I**magine and **Co**mmunications in **M**edicine – a standard for transfering digital imagine data and communication between medical devices.
DirectX	A collection of APIs for handling tasks related to multimed on Microsoft platforms.
DVD	**D**igital **V**ersatile **D**isc or **D**igital **V**ideo **D**isc is a digital optical disc storage format and pjysical media.
EdgePort	An USB-to-RS232 converter
ESS	Shortcut for **ESS**ential
Firewire	IEEE 1394 aka FireWire is an interface standard for hig-speed serial communication
FP6000	**F**lash**p**oint 6000, name of the Stryker Navigation Camera used in the the NAV3i Platform Family
I/O	**I**nput/**O**utput
LED	**L**ight-**E**mitting-**D**iode
MR	**M**agentic **R**esonance imagine technique

Term	Definition
OS	**O**perating **S**ystem
PCI, PCIe	**P**eripheral **C**omponent **I**nterconnect, an industry-standard bus for attaching peripherals to computers. The suffix "e" is used for PCI Express, the successor of conventional PCI.
PDF	**P**ortable **D**ocument **F**ormat, an open standard for document exchange
RC	**R**isk-**C**ontrol
RFID	**R**adio **F**requency **I**dentification, a technology for exchanging data using electromagnetic waves
SFB	**S**tryker-**F**irewire-**B**us, an properitary protocol for serial communication via Firewire (IEEE 1394) used for communication between computer and Sryker Navigation Camera
SOUP	**S**oftware of **U**nknown **P**rovenance, a software item that is already developed and generally available and that has not been developed for the purpose of being incorporated into the Medical Device (also known as “off-the-shelf software”) or software previously developed for which adequate records of the development Processes are not available.
UPS	**U**ninterruptible **P**ower **S**upply
USB	**U**niversal **S**erial **B**us, a common bus system for transferring data
X Protocol	The X Window System core protocol
X Server	A server implementing the X Protocol
X11	The latest major version of the X Protocol

65 For more project-specific definitions and acronyms refer to the Design Inputs [DI_NAV3], [DI_NAV3I] and [DI_NAVSUITE3].

1.4 References

ID	Title	Rev.*	Doc. No.
SADD_NAV3	SADD - NAV3i Platform Family - ADAPT / NAV3 (#0000010743,NavSystem III)	Auto	0000004229
SADD_NAV3I	SADD - Navigation System III - NAV3i (#0000011363,NAV3i)	Auto	0000014409
SADD_NAVSUITE3	SADD - NAV3i Platform Family - NavSuite3 (#0000012123,NavSuite3)	Auto	0000040549
DS_OS	DS - Nav3i Platform Family - SPC 3.1 Operating System V2 (#0000012124,SPC3.1)	Auto	0000039082
DI_NAV3	DI - NAV3i Platform Family - ADAPT / NAV3 (#0000010743,NavSystem III)	Auto	0000006309
DI_NAV3I	DI - NAV3i Platform Family - NAV3i (#0000011363,NAV3i)	Auto	0000014207
DI_NAVSUITE3	DI - NAV3i Platform Family - NavSuite3 (#0000012123,NavSuite3)	Auto	0000039104
SOUP_WIN8	SOUP - Windows Embedded 8.1 Industry Pro 64-Bit Basisimage AA.00 - SW-IM-00001154 001-AA (#0000010162,Software Components)	Auto	0000041919
SOUP_ADOBE	SOUP - Adobe Reader 11 (#0000010162,Software Components)	Auto	0000041823

ID	Title	Rev.*	Doc. No.
SOUP_RFID1	SOUP - ASKCPL 407 driver 2.4.6.0 (#0000010162,Software Components)	Auto	0000041913
SOUP_RFID2	SOUP - Elatec TWN4 RFID reader driver 5.3.0.6 (#0000010162,Software Components)	Auto	0000041912
SOUP_GRB	SOUP - Terratec G3 Driver 2.07.0621.00 (#0000010162,Software Components)	Auto	0000041915
SOUP_AXEDA	SOUP - Axeda Connector and Desktop Server 6.6 (#0000010162,Software Components)	Auto	0000041914
SOUP_CANUSB	SOUP - CanUSB Driver 6.2.2.92 (#0000010162,Software Components)	Auto	0000041824
SOUP_EDGE	SOUP - EdgePort Driver 5.70.105.0 (#0000010162,Software Components)	Auto	0000041825
SOUP_NVIDIA	SOUP - NVIDIA Quadro Professional Driver v347.52 (#0000010162,Software Components)	Auto	0000043708
SOUP_UPSMAN	SOUP - UPS-Management Software V5.9.95 (#0000010162,Software Components)	Auto	0000041918
SRS_APM	SRS - Application Manager 5.0 (#0000010381,Application Manager)	Auto	0000041730
SADD_APM	SADD - Application Manager - 5.0 (#0000010381,Application Manager)	Auto	0000041739
SDD_SFB	SDD_SFBHostInterface (#0000012190,Win8 SFB Driver)	Auto	0000022259
BP_OS	Design Freeze OS (#0000012124,SPC3.1)	Auto	0000042408
DIOTV_NAV3I	DIOTV - Navigation System III - NAV3i (#0000011363,NAV3i)	Auto	0000014589
DIOTV_NAV3	DIOTV NavBasic NavPlus (#0000010743,NavSystem III)	Auto	0000012392
DIOTV_NAVSUITE3	DIOTV - NAV3i Platform Family - NavSuite3 (#0000012123,NavSuite3)	Auto	0000040903
RA_NAV3	RM - NavSystem III - Nav Basic / Nav Plus (#0000010743,NavSystem III)	Auto	0000004223
RA_NAV3I	RM - Navigation System III - NAV3i (#0000011363,NAV3i)	Auto	0000014214
RA_NAVSUITE3	RM - Navigation System III - NavSuite3 (#0000012123,NavSuite3)	Auto	0000039106
RARC_NAV3	RARC - NAV3i Platform Family - ADAPT / NAV3 (#0000010743,NavSystem III)	Auto	0000011995
RARC_NAV3I	RARC - Navigation System III - NAV3i (#0000011363,NAV3i)	Auto	0000014215
RARC_NAVSUITE3	RARC - NAV3i Platform Family - NAVSuite3 (#0000012123,NavSuite3)	Auto	0000039402

ID	Title	Rev.*	Doc. No.
RARC_CRN	Risk Assessment - Cranial 2.0 - Cranial/ENT/CMF 2.0 (#0000010963,Cranial 2.0)	Auto	0000014769

*Auto: Document's revision number is updated automatically by OfficeTrace.

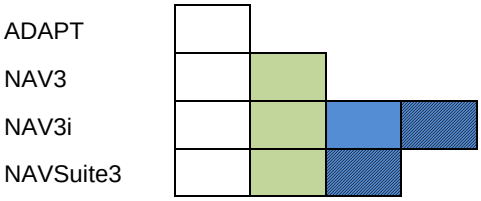
2 System Context

This chapter defines the borders between the NAV3i Operating System and its neighboring hardware and software components. It identifies all external interfaces between those. For a complete system overview, refer to the [SADD_NAV3: SADD - NAV3i Platform Family - ADAPT / NAV3], [SADD_NAV3I: SADD - Navigation System III - NAV3i], [SADD_NAVSUITE3].

The NAV3i Operating System runs on the SPC-3 computer of the NAV3i Platform Family. The family consist of ADAPT, NAV3, NAV3i and the NAVSuite3.

The following picture shows the different platform configurations. Many components are shared with all members of the platform family. Some components are marked with colors which represent the differences between the platform configurations.

Platform Configurations

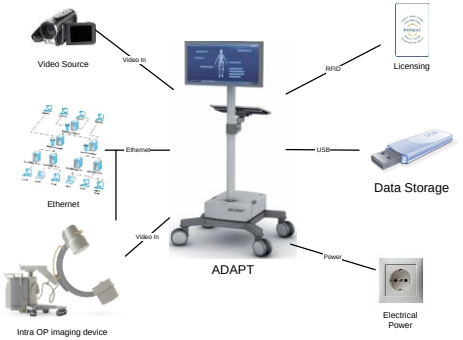


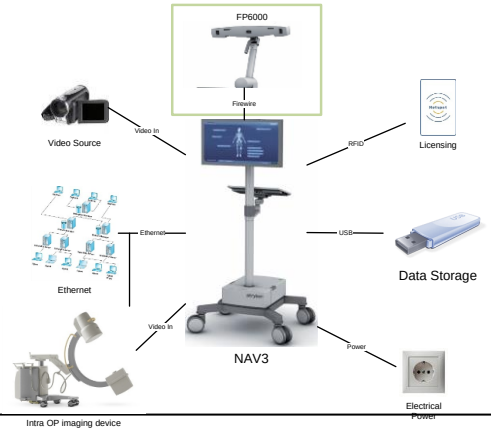
Color	Scope
White	Component is used by all platforms of the NAV3i Platform Family
Green	Component is used by platforms using the Stryker Navigation Camera
Blue	Component is used by NAV3i platform only
Blue-checked	Component may be used by platforms supporting microscope integration

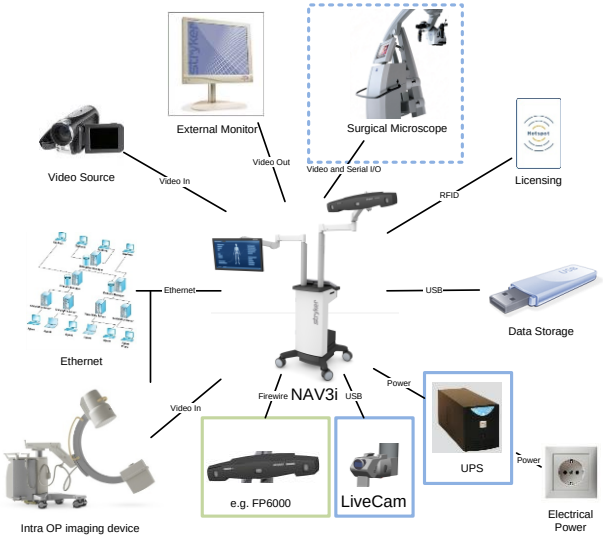
stryker

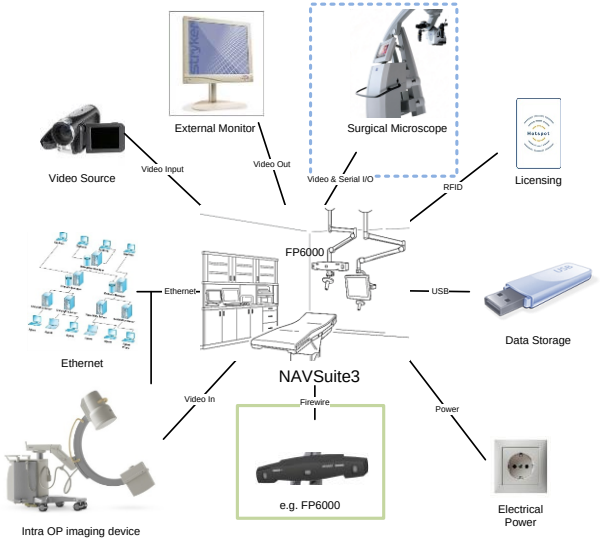
F 35-005/ Version B

90

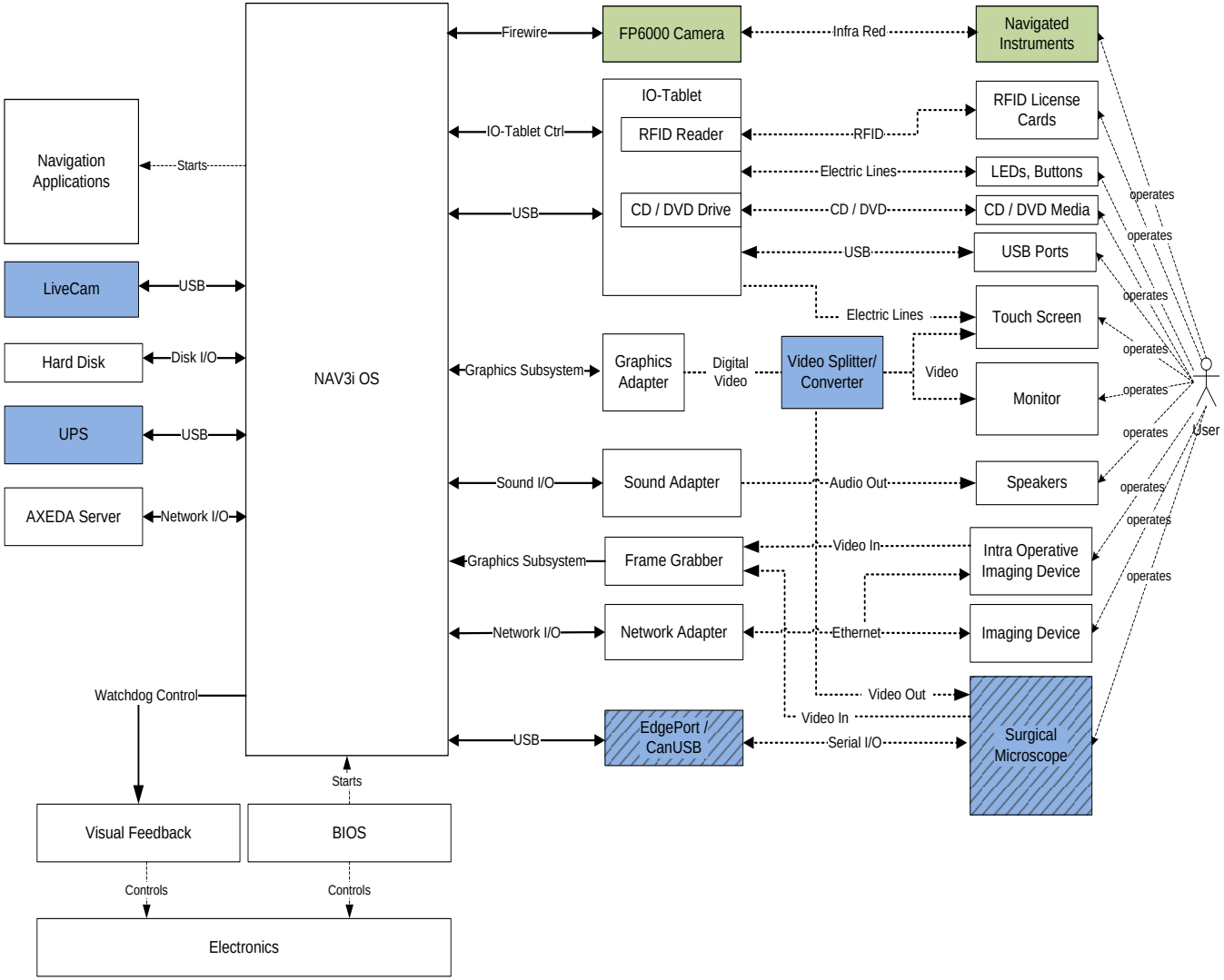








The following diagram shows a schematic representation of all components of the NAV3i Platform Family which interacts directly or indirectly with the NAV3i Operating System.



2.1 Configuration Management

The NAV3i Operating System shall be the same for all platforms of the NAV3i Platform Family (ADAPT, NAV3, NAV3i and NAVSuite3).

To meet the requirements for the different platforms the NAV3i Operating System will be configured upon installation. The configuration will activate/deactivate services and drivers which are used/not used for the platform to be installed.

Please refer to [DS_OS] for the requirement.

2.2 Neighbouring Systems

ID	Neighbouring System	Description
NS1	**Navigation Applications**	Software components implementing clinical use cases. They are not part of the NAV3i Operating System.
NS2	**Visual Feedback**	Hardware component monitoring the reaction time of the operating system. When the NAV3i Operating System does not trigger the watchdog on time, the user is notified.
NS3	**BIOS**	Low level software enabling access to the electronics.
NS4	**Electronics**	Electronic components of the computer system as identified in [SADD_NAV3: SADD - NAV3i Platform Family - ADAPT / NAV3], [SADD_NAV3I: SADD - Navigation System III - NAV3i], [SADD_NAVSUITE3]. Some of these components play an important role in the context of this SADD and are also listed below.
NS5	**FP6000 Camera**	Stryker Navigation camera used to localize the Stryker Navigated Instruments.
NS6	**Navigated Instruments**	Application-specific instruments providing functionality of wireless position tracking, used by the surgeon for navigated surgery. Navigated instruments could be a pointer, patient tracker, etc.
NS7	**RFID License Cards**	RFID cards holding information about licensing software applications.
NS8	**IO-Tablet**	Hardware component providing a visual output device, a touch screen for user input and several data transfer devices. It mainly consists of the components RFID Reader, LEDs, Buttons, USB Ports, CD/DVD Drive and Touch Screen (listed below).
NS9	**RFID Reader**	RFID reader, used to read from and write to [NS7: RFID License Cards].
NS10	**LEDs, Buttons**	LEDs signalling status information to the user and buttons used for user interaction.
NS11	**USB Ports**	External USB ports to connect USB sticks etc.
NS12	**CD / DVD Drive**	CD/DVD drive for data import / export.
NS13	**Touch Screen**	Monitor providing capacitive touch.
NS14	**Graphics Adapter**	Hardware device responsible for displaying information on screens.
NS15	**Video Splitter / Converter**	Hardware device responsible for splitting the video signal from the graphics adapter. May also include a conversion of the video signal.
NS16	**Sound Adapter**	Hardware device responsible for creating audio signals.
NS17	**Speakers**	Monitor with speakers for audible feedback.
NS18	**Hard Disk**	Hardware device responsible for storing data permanently.
NS19	**Frame Grabber**	Hardware device responsible for capturing a video stream.
NS20	**Network Adapter**	Hardware device responsible for transferring data to and from the network (cable bound LAN or wireless LAN).
NS21	**EdgePort / CanUSB**	Hardware devices responsible for connection to microscopes.

ID	Neighbouring System	Description
NS22	**LiveCam**	Optical camera rigidly mounted to the camera arm.
NS23	**UPS**	Uninterruptable power supply.
NS24	**AXEDA Server**	A server where system information about the system are collected and users may remotely connect to the system and watch screen output and forward keyboard and mouse input.
NS25	**Intra Operative Imaging Device**	A scanner (CT, MR, C-Arm) acquiring intra-operative images.
NS26	**Image Device**	A scanner (CT, MR, C-Arm) acquiring pre-operative images.
NS27	**Surgical Microscope**	A navigated microscope providing remote control buttons and video injection.

2.3 External Interfaces

ID	Interface	Description	Satisfies	Design Spec.
IF1	**Watchdog Control**	Hardware interface, used by the Operating System in order to enable, disable and trigger the Hardware Watchdog.	[DIOTV_NAV3I] [DIOTV_NAV3] [DIOTV_NAVSUITE3]	Internal design documentation at supplier ads-tec
IF2	**Firewire**	Software interface (Windows API), used to communicate with the Stryker Navigation camera.	[DIOTV_NAV3I] [DIOTV_NAV3] [DIOTV_NAVSUITE3]	Windows API
IF3	**IO-Tablet Ctrl**	Software interface (ads-tec API), used to interface with buttons and LEDs on the IO-Tablet.	[DIOTV_NAV3I] [DIOTV_NAV3] [DIOTV_NAVSUITE3]	Internal design documentation at supplier ads-tec
IF4	**Graphics Subsystem**	Software interface (Windows API), used to communicate with the Graphics Adapter.	[DIOTV_NAV3I] [DIOTV_NAV3] [DIOTV_NAVSUITE3]	Windows API
IF5	**Disk I/O**	Software interface (Windows API), used to communicate with mass storage devices.	[DIOTV_NAV3I] [DIOTV_NAV3] [DIOTV_NAVSUITE3]	Windows API
IF6	**Sound I/O**	Software interface (Windows API), used to communicate with the Sound Adapter.	[DIOTV_NAV3I] [DIOTV_NAV3] [DIOTV_NAVSUITE3]	Windows API
IF7	**Network I/O**	Software interface (Windows API), used to communicate with the Network Adapter.	[DIOTV_NAV3I] [DIOTV_NAV3] [DIOTV_NAVSUITE3]	Windows API
IF8	**USB**	Generic software interface (Windows API), used to communicate with several different hardware devices	[DIOTV_NAV3I] [DIOTV_NAV3] [DIOTV_NAVSUITE3]	Windows API

3 System Decomposition

105 This chapter breaks down the system into individual hardware and software units.

3.1 Hardware Decomposition

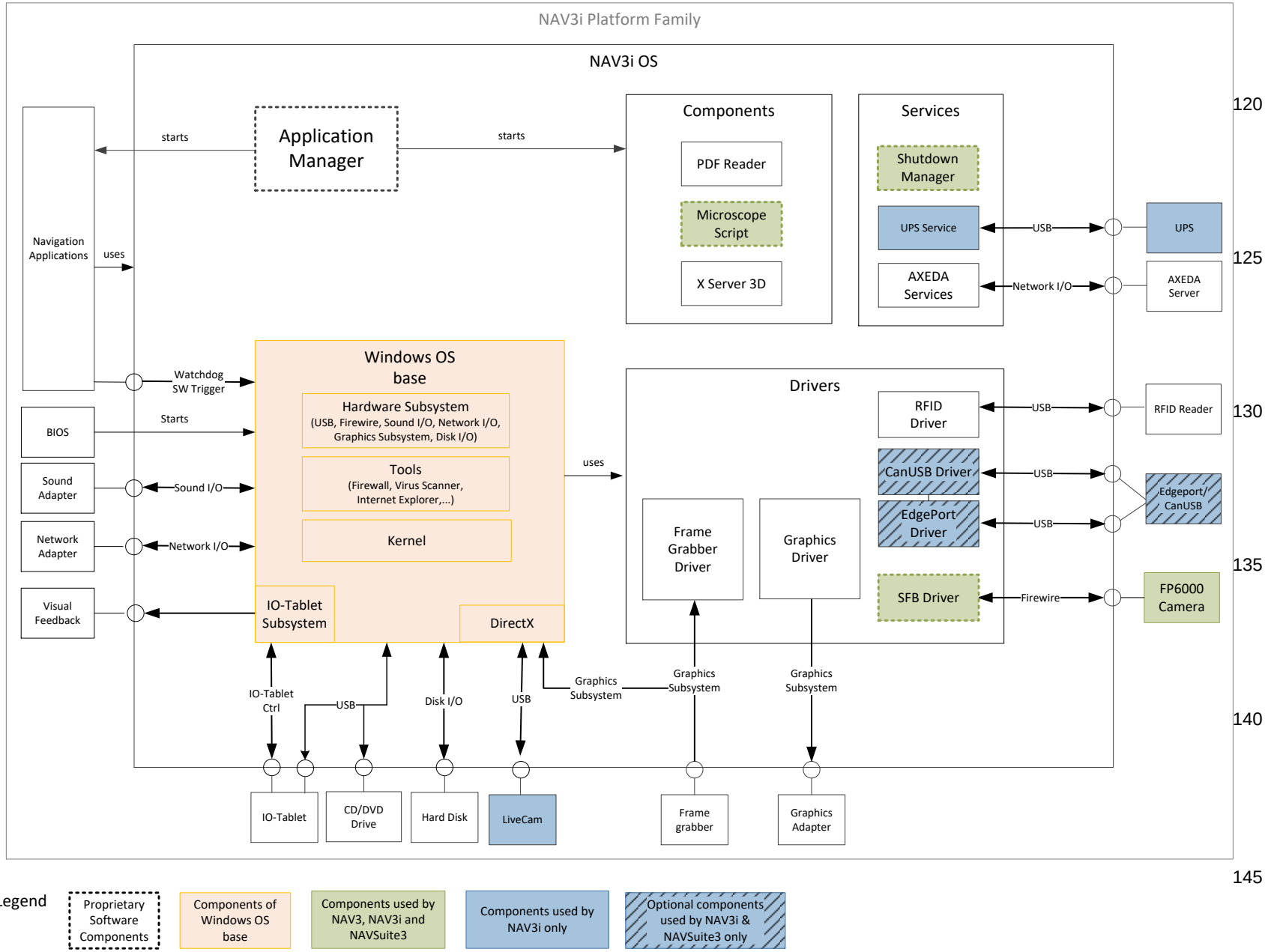
Refer to [SADD_NAV3: SADD - NAV3i Platform Family - ADAPT / NAV3], [SADD_NAV3I: SADD - Navigation System III - NAV3i], [SADD_NAVSUITE3].

3.2 Software Decomposition

3.2.1 Overall Software System

The NAV3i Operating System is the common software platform for Navigation Applications.

The system is based on a pre-configured Windows operating system and includes a number of additional 3rd party components (SOUPs) and a number of components developed by Stryker Navigation. For further details on SOUPs refer to chapter 6, SOUP – Software Of Unknown Provenance. More information about the NAV3i Operating System can be found in [DS_OS].



Legend

- Proprietary Software Components
- Components of Windows OS base
- Components used by NAV3, NAV3i and NAVSuite3
- Components used by NAV3i only
- Optional components used by NAV3i & NAVSuite3 only

3.2.1.1 Proprietary Software Components

ID	SW Unit	Description	Safety Class	Satisfies	Design Spec.
SW1	Application Manager	Software to select and start Navigation Applications and to provide functions for administrative tasks. • Provides a user interface for the nurse/surgeon to start Navigation Applications installed on the Navigation System. • Provides a user interface for the system administrator for common administrative tasks. • Provides maintenance and testing tools for the navigation hardware. • Supports Navigation licensing mechanisms for logistic reasons.	A	[DIOTV_NAV3I] [DIOTV_NAV3] [DIOTV_NAVSUITE3]	[DIOTV_NAV3I] [DIOTV_NAV3] [DIOTV_NAVSUITE3]
SW2	SFB Driver	Driver software for the Stryker FireWire Bus. Provides an API used by Navigation Applications to communicate with the Stryker Navigation camera. The version of the SFB driver is 6.25.	A	[DIOTV_NAV3I] [DIOTV_NAV3] [DIOTV_NAVSUITE3]	[DIOTV_NAV3I] [DIOTV_NAV3] [DIOTV_NAVSUITE3]
SW7	Microscope Scripts	Scripts that are used to initialize display output for use with microscopes.	A	[DIOTV_NAV3I] [DIOTV_NAVSUITE3]	[DIOTV_NAV3I] [DIOTV_NAVSUITE3]
SW16	Shutdown Manager	A Service that handles a defined shutdown of the system. It is either triggered by the IO-Tablet Subsystem in case of an hardware power down or by the Application Manager in case a power down is requested by the Application Manager.	A	[DIOTV_NAV3I] [DIOTV_NAV3] [DIOTV_NAVSUITE3]	[DIOTV_NAV3I] [DIOTV_NAV3] [DIOTV_NAVSUITE3]
SW17	OS Scripts	Collection of batch scripts configuring the system. Some scripts are run on user's logon, some at logoff and some may be run on user's request.	A	[DIOTV_NAV3I] [DIOTV_NAV3] [DIOTV_NAVSUITE3]	[DIOTV_NAV3I] [DIOTV_NAV3] [DIOTV_NAVSUITE3]

3.2.1.2 3rd Party Software Components (SOUP)

ID	SW Unit	Description	Safety Class	Satisfies	Design Spec.
SW3	Windows OS base	Pre-configured Windows 8.1 Embedded Industry Pro; provides standard functionality of Microsoft Windows 8.1 and additionally contains drivers and services in order to fully	C	[DIOTV_NAV3I] [DIOTV_NAV3] [DIOTV_NAVSUITE3]	[DIOTV_NAV3I] [DIOTV_NAV3] [DIOTV_NAVSUITE3]

ID	SW Unit	Description	Safety Class	Satisfies	Design Spec.
		support all platforms of the NAV3i Platform Family. For details of the exact Windows configuration refer to [SOUP_WIN8].			
SW4	RFID Driver	Driver software for the RFID reader; provides an API, which is used by Application Manager. See [SOUP_RFID1] and [SOUP_RFID2], depending on the used IO-Tablet generation	A	[DIOTV_NAV3I] [DIOTV_NAV3] [DIOTV_NAVSUITE3]	[DIOTV_NAV3I] [DIOTV_NAV3] [DIOTV_NAVSUITE3]
SW5	Frame Grabber Driver	Driver software for frame grabber card to receive analog video input. See [SOUP_GRB]	A	[DIOTV_NAV3I] [DIOTV_NAV3] [DIOTV_NAVSUITE3]	[DIOTV_NAV3I] [DIOTV_NAV3] [DIOTV_NAVSUITE3]
SW6	Graphics Driver	Driver software for Nvidia graphics cards. See [SOUP_NVIDIA]	C	[DIOTV_NAV3I] [DIOTV_NAV3] [DIOTV_NAVSUITE3]	[DIOTV_NAV3I] [DIOTV_NAV3] [DIOTV_NAVSUITE3]
SW8	PDF Reader	Software to display PDF documents (such as user manuals) on screen. See [SOUP_ADOBE]	A	[DIOTV_NAV3I] [DIOTV_NAV3] [DIOTV_NAVSUITE3]	[DIOTV_NAV3I] [DIOTV_NAV3] [DIOTV_NAVSUITE3]
SW9	Virus Scanner	Software to protect the system against malicious software. This software unit is a component of [SW3].	A	[DIOTV_NAV3I] [DIOTV_NAV3] [DIOTV_NAVSUITE3]	[DIOTV_NAV3I] [DIOTV_NAV3] [DIOTV_NAVSUITE3]
SW10	UPS Service	Control software for the uninterruptible power supply (UPS). It informs the user if the connection to electrical power got lost and the system is running on battery. It also informs the user if battery power is getting low. See [SOUP_UPSMAN]	A	[DIOTV_NAV3I]	[DIOTV_NAV3I]
SW11	CanUSB Driver	Driver that handles the communication via CAN bus between navigation application and microscope. See [SOUP_CANUSB]	A	[DIOTV_NAV3I] [DIOTV_NAVSUITE3]	[DIOTV_NAV3I] [DIOTV_NAVSUITE3]
SW12	EdgePort Driver	Driver that handles the communication via EdgePort between navigation application and microscope. See [SOUP_EDGE]	A	[DIOTV_NAV3I] [DIOTV_NAVSUITE3]	[DIOTV_NAV3I] [DIOTV_NAVSUITE3]
SW13	AXEDA Services	Services to send system information to a remote server and to provide desktop remote access.	A	[DIOTV_NAV3I] [DIOTV_NAVSUITE3]	[DIOTV_NAV3I] [DIOTV_NAVSUITE3]

ID	SW Unit	Description	Safety Class	Satisfies	Design Spec.
		See [SOUP_AXEDA]			
SW15	Firewall	The Firewall is used to protect the system from attacks from external networks. This software unit is a component of [SW3].	A	[DIOTV_NAV3I] [DIOTV_NAV3] [DIOTV_NAVSUITE3]	[DIOTV_NAV3I] [DIOTV_NAV3] [DIOTV_NAVSUITE3]

4 Software Safety Classification

This chapter assigns a safety class (A, B, or C, in accordance to IEC 62304) to the system as a whole and the software units into which it is decomposed. For each classification which is lower than C a rationale is given.

The safety classes have the following meaning:

- Class A: No injury or damage to health is possible (minor level of concern)
- Class B: Non-serious injury is possible (moderate level of concern)
- Class C: Death or serious injury is possible (major level of concern)

The following table presents a list of common potential hazards, which are related to software malfunctions:

Hazard	Harm	Severity	Safety Class
Display of a wrong navigational information	Treatment of a wrong location	S4	C – Major level of concern
Unavailability of the navigation system detected during surgery	Abortion of surgery after patient is anesthetized.	S3	B – Moderate level of concern
Major malfunction or flaw of the system which gets resolved during surgery after 15min.	OR time extension > 15min	S2	B – Moderate level of concern
Minor malfunction or flaw of the system which gets resolved during surgery within 15min	OR time extension <= 15min	S1	A – Minor level of concern
Unavailability of the navigation system detected prior to surgery before patient is prepared.	No harm.	S0	A – Minor level of concern

4.1 Overall Safety Class

The software system NAV3i Operating System is assigned to safety class C. The overall software system safety classification for the NAV3i Operating System is also documented in [RA_NAV3], [RA_NAV3I] and [RA_NAVSUITE3].

The NAV3i Operating System is not a standalone product. It is used as the common software platform for all Navigation Applications and thus is part of any Navigation Application, which runs on this platform. Therefore the risks and harms for the NAV3i Operating System need to be discussed in context of the risks and harms associated with the Navigation Application running on the system.

The Navigation Application associated with the highest software risk is represented by the CranialMap Navigation Application. The safety class of CranialMap is C, derived from the maximal possible harm of treatment of a wrong location (S4).

There are some components in the NAV3i Operating System which can directly contribute to this harm. **Therefore the overall safety classification for the NAV3i Operating System is set to “C” (major level of concern).**

4.2 Component Safety Classes

Most software components do not contribute to the risks and harms mentioned in the previous section and therefore can be assigned lower safety classes than the overall system’s safety class. The following table provides a risk assessment

and safety classification for each of the software components, which is part of the NAV3i Operating System, and discusses how this software component could possibly contribute to harm.

175

SW Unit ID	SW Unit	Safety Class	Rationale for Lower Safety Classification
[SW1]	Application Manager	A	The Application Manager is the “welcome screen” which appears, when the user logs into the system. Its main function is to perform a license check and start the Navigation Applications as selected by the user. A malfunction of the Application Manager, which is not launching the Navigation Application, would be detected at installation time and does not impose any harm to the patient. Other functions of the application manager are administrative functions only and do not impose any harm to the patient as well.
[SW2]	SFB Driver	A	The SFB Driver implements the communication protocol between the Navigation Applications and the Navigation Camera. It does not calculate any positional information, but purely realizes the data transport layer. The SFB driver is used during navigated surgery. Malfunction of the SFB Driver would lead to connection loss to camera and causing the navigation to stop working. The Navigation Applications indicate this failure mode to the user by displaying an error message. If this failure mode occurs, in worst case, a restart of the application or the computer system would reinitialize the SFB Driver and resolve the problem. The system and the Navigation Applications are specified to restart within a couple of minutes (in any case < 15min). Thus malfunction of the SFB Driver would lead to an OR time extension of < 15min.
[SW3]	Windows OS base	C	The Windows Operating System provides the common basis for all software running on a PC. Malfunction of the operating system may permanently make the system unavailable (e.g. caused by unauthorized access or malware attack to the system). The system may stop working and its function may not be available anymore for surgery. The user cannot use the system for navigated surgery. [RARC_NAV3I.R18], [RARC_NAV3I.R36] Malfunction of the operating system is very unlikely to directly result in wrong calculations of the navigation information displayed on screen. However the operating system can cause the system to perform slowly or causing the system to halt. A system halt or very slow update rate of the navigated images during surgery, which is not recognized by the user, can lead to wrong navigation information and thus a treatment of a wrong location. [RARC_NAV3I.R26], [RARC_NAV3I.R28] Malfunction of the operating system may permanently make the system unavailable (e.g. caused by unauthorized access or malware attack to the system). Because of this it may be impossible to prepare the system for surgery or to access the patient data. The user cannot use the system for navigated surgery. [RARC_NAV3I.R33], [RARC_NAV3I.R34] Malfunction of the operating system is very unlikely to directly result in wrong display of video images. However the operating

SW Unit ID	SW Unit	Safety Class	Rationale for Lower Safety Classification
			system can cause system performance issues or malfunction which forbids display of video images on screen. [RARC_NAV3I.R49]
[SW4]	RFID Driver	A	The RFID driver is used by Application Manager only. The driver represents software interface [NS9: RFID Reader]. Malfunction of the driver would lead to non-acceptance of the license card and would be detected prior to surgery and could be resolved through system reboot.
[SW5]	Frame Grabber Driver	A	The Frame Grabber Driver is responsible for receiving images from the analog video input. Malfunction of the Frame Grabber Driver would most likely result in non-availability of those images. This failure mode is easily detected by the user. A system reboot would resolve the situation. The Navigation Applications are designed in a way that a full reboot cycle does not take longer than 30 minutes, which results in a hazard of minor malfunction or flaw of the system which gets resolved during surgery.
[SW6]	Graphics Driver	C	The Graphics Driver is the driver software for the NVidia Graphics Card Its main responsibility is displaying information on the screen. Malfunction of the Graphics Driver is very unlikely to directly result in wrong calculations of the navigation information displayed on screen. However the Graphics Driver can cause the display to perform slowly or causing a frozen screen. A frozen screen or very slow update rate of the navigated images during surgery, which is not recognized by the user, can lead to a wrong navigation information display and thus a treatment of a wrong location. [RARC_NAV3I.R26], [RARC_NAV3I.R28]
[SW7]	Microscope Script	A	The script set consists of scripts that initialize the system so that a microscope can be used. Malfunction of the scripts would lead to connection loss to non-availability of the microscope heads up display. The scripts are executed once during Microscope installation. A malfunction would be detected during installation. The resulting hazard is unavailability of the navigation system detected prior to surgery before patient is prepared.
[SW8]	PDF Reader	A	The PDF Reader is used to display user manuals or surgery reports. Failure of this software component would result in non-availability of the user manual or surgery reports. In typical use the user manual is not consulted during surgery. The surgery reports are created and displayed at the end of a surgery for documentation purposes only. Malfunction of the PDF Reader does not result in any harm to patient or the user.
[SW9]	Virus Scanner	A	The Virus Scanner is used to protect the system from malware. There is a potential risk that the virus scanner could slow down the performance of the computer system. The essential performance of the system would be compromised if the performance degradation would lead to a frame rate larger than 4 sec per frame. The usual update rates

SW Unit ID	SW Unit	Safety Class	Rationale for Lower Safety Classification
			of the Navigation Applications lie typically at <0.2 sec per frame. That means essential performance would be compromised if the Virus Scanner would degrade the system performance by a factor of 4 / 0.2 = 20. Automatic updates of the virus scanner definitions are disabled. Thus, a slowdown of the system performance by factor 20 due to virus scanner activities is very unlikely.
[SW10]	UPS Service	A	The UPS service is used to control the hardware of the uninterruptible power supply. The UPS controller software is a convenience feature (e.g. to move the Navigation System from one room to another without shutdown). The power supplied by the internal batteries lasts for a couple of minutes. During surgery the system is always connected to an external power supply. Malfunction of the UPS service would mean that this feature is not available and does not impose any risk to the patient.
[SW11]	CanUSB Driver	A	The CanUSB Driver implements the communication protocol between the Navigation Applications and CAN USB compatible surgical microscopes. It does not calculate any positional information on its own, but purely realizes data transport layer. The CanUSB driver is used during navigated surgery. Malfunction of the CanUSB Driver would lead to connection loss to the microscope and leading to non-availability of the microscope heads up display and the ability to control the Navigation Application through the buttons of the microscope. In that case a restart of the computer system would restart the CanUSB Driver and resolve the problem. The NAV3i Operating System and the Navigation Applications are specified to restart within a couple of minutes (in any case < 10min). Thus malfunction of the CanUSB Driver would lead to an OR Time extension of < 10min.
[SW12]	EdgePort Driver	A	The EdgePort Driver implements the communication protocol between the Navigation Applications and EdgePort compatible surgical microscopes. It does not calculate any positional information on its own, but purely realizes data transport layer. The EdgePort driver is used during navigated surgery. Malfunction of the EdgePort Driver would lead to connection loss to the microscope and leading to non-availability of the microscope heads up display and the ability to control the Navigation Application through the buttons of the microscope. In that case a restart of the computer system would restart the EdgePort Driver and resolve the problem. The NAV3i Operating System and the Navigation Applications are specified to restart within a couple of minutes (in any case < 10min). Thus malfunction of the EdgePort Driver would lead to an OR Time extension of < 10min.
[SW13]	AXEDA Services	A	The AXEDA Services provide the possibility of remote maintenance through remote desktop access, which allows a Stryker Technician to perform system maintenance without travelling to the hospital. Malfunction of the AXEDA Services shortly before or during surgery could stop the local user from accessing the patient

SW Unit ID	SW Unit	Safety Class	Rationale for Lower Safety Classification
			data [RARC_NAV3I.R14] or stop the system at all [RARC_NAV3I.R37].
[SW15]	Firewall	A	The Firewall is used to protect the system against unauthorized access and/or malware. There is a potential risk when network ports are closed which are necessary for applications to import DICOM data. In such a case an alternative DICOM import can be chosen which would lead to an OR time extension <30 minutes.
[SW16]	Shutdown Manager	A	The Shutdown Manager is used to shut down the system. It displays a message box with choices what to do. Malfunction of the Shutdown Manager would result in either the system cannot be shut down or the message box is displayed. If the system cannot be shut down it would not lead to a risk because this is done at the end of a procedure and no patient would be involved. If the message box is displayed the user has the option to cancel the shutdown and even to but the dialog into the background. In every case the result is user annoyance only.
[SW17]	OS Scripts	A	Malfunction of any of the scripts will not result in in-availability of the system for surgery or missing or wrong display of images: • defenderupdate.bat: *updates virus scanner on login* • display_init.bat + helper scripts: *sets display profile on login* • start_set_display_settings.bat: *runs display_init.bat manually from Application Manager* • disable_auto_signin.bat: *disables auto-login on system shutdown for next system start* • rc_dis.bat / rc_ena.bat: *disables or enables remote keyboard and mouse on login / logout* • fp6powerup.bat: *boots FP6000* • wifi_on.bat / wifi_off.bat: *enables / disables WLAN service from Application Manager* None of these scripts has any effect on the software packages which implement the medical applications.

5 Software Risk Control

The following table summarizes for each class B or C SOUP all risk controls which mitigate the hazards identified in the previous section.

All risk controls have been defined in the corresponding risk management file of ADAPT/NAV3, NAV3i and the NAVSuite3
180 ([RARC_NAV3], [RARC_NAV3I], [RARC_NAVSUITE3].
Risk assessment concerning Software is identical in the above mentioned risk management files. All Software RCs have the same ID, so in the table below only the RC number is mentioned.

For each software unit a re-assessment of the residual risk after implementation of the risk controls is provided.

Reference to SW Unit	Safety Class Before Risk Controls	Risk Controls	Safety Class After Risk Controls
[SW3: Windows OS base]	C	In order to prevent system freeze conditions or conditions of severe performance loss the following risk controls have been implemented in the NAV3i Operating System: The operating system is protected against unauthorized use: • [RARC_NAV3I.RC80: System shall provide password protection for user log in] The operating system is secured against software updates, which leave the system in a non-validated state: • [RARC_NAV3I.RC81: A firewall and a Virus Scanner shall be installed and activated] • [RARC_NAV3I.RC82: Automatic updates of the system shall be deactivated] BIOS settings are secured against unintended changes due to battery power loss: • [RARC_NAV3I.RC93: The BIOS setting shall be protected by password] • [RARC_NAV3I.RC120: BIOS settings are maintained as specified after BIOS battery power loss.] BIOS version number, Operating system version number, Reliability of PC and Framegrabber version have the status of a Critical Quality Attribute: • [RARC_NAV3I.CQA2: BIOS version] • [RARC_NAV3I.CQA3: Stryker OS version] • [RARC_NAV3I.CQA6: Reliability of PC (no system freeze / crash)] • [RARC_NAV3I.CQA19: Framegrabber, version] In addition to the risk controls implemented by the NAV3i Operating System the CranialMap software implements the following risk controls for detection of screen freeze conditions: • [RARC_CRN.RC1370: The system is designed to constantly display tool visibility information and updates the screen during navigation. This signalizes system activity.] • [RARC_CRN.RC1375: The system signalizes activity during navigation by displaying a heartbeat which changes periodically. If the system freezes during navigation the heartbeat stops changing.]	A
[SW6: Graphics Driver]	C	In order to prevent system freeze conditions or conditions of severe performance loss the following risk controls have been implemented in the NAV3i Operating System: The operating system is protected against unauthorized use prohibiting manual software changes to the Graphics Driver: • [RARC_NAV3I.RC80: System shall provide password protection for user log in] The operating system is secured against software updates, which leave the system in a non-validated state: • [RARC_NAV3I.RC81: A firewall and a Virus Scanner shall be installed and activated] • [RARC_NAV3I.RC82: Automatic updates of the system shall be deactivated] BIOS settings are secured against unintended changes:	A

Reference to SW Unit	Safety Class Before Risk Controls	Risk Controls	Safety Class After Risk Controls
		• [RARC_NAV3I.RC93: The BIOS setting shall be protected by password] Graphics Card version has the status of a Critical Quality Attribute: • [RARC_NAV3I.CQA1: Graphicscard Model and Version] In addition to the risk controls implemented by the NAV3i Operating System the CranialMap software implements the following risk controls for detection of screen freeze conditions: • [RARC_CRN.RC1370: The system is designed to constantly display tool visibility information and updates the screen during navigation. This signalizes system activity.] • [RARC_CRN.RC1375: The system signalizes activity during navigation by displaying a heartbeat which changes periodically. If the system freezes during navigation the heartbeat stops changing.]	

6 SOUP – Software Of Unknown Provenance

The following table lists all software items which are considered software of unknown provenance (SOUP).

Reference to SW Unit	Version	Manufacturer	Reference to SOUP Description
[SW3: Windows OS base]	AA.00	ads-tec GmbH	[SOUP_WIN8]
[SW4: RFID Driver] (*)	2.4.6.0	ASK	[SOUP_RFID1]
	5.3.0.6	Elatec gmbH	[SOUP_RFID2]
[SW5: Frame Grabber Driver]	2.7.621.0	Terratec	[SOUP_GRB]
[SW6: Graphics Driver]	V347.52	NVidia	[SOUP_NVIDIA]
[SW8: PDF Reader]	11.0.0	Adobe	[SOUP_ADOBE]
[SW10: UPS Service]	5.9.95	Effekta	[SOUP_UPSMAN]
[SW11: CanUSB Driver]	6.2.2.92	Softing	[SOUP_CANUSB]
[SW12: EdgePort Driver]	5.70.105.0	Digi International	[SOUP_EDGE]
[SW13: AXEDA Services]	6.6	Axeda	[SOUP_AXEDA]

* Note: depending on the IO-Tablet version [SOUP_RFID1] or [SOUP_RFID2] driver is used.

7 Deployment View

Refer to [3.2.1]

8 Runtime View

No architectural runtime aspects.

9 Architectural Key Aspects

This chapter describes general architectural aspects which aren't addressed so far or could not be assigned to one single system unit.

9.1 Safety

No further architectural safety requirements except those already listed in in [DI_NAV3], [DI_NAV3I], [DI_NAVSUITE3] and [RARC_NAV3], [RARC_NAV3I] and [RARC_NAVSUITE3].

ID	Technical Requirement	Acceptance Criteria	ESS.	Satisfies	Verification Means
n/a	n/a	n/a	n/a	n/a	n/a

9.2 Accuracy

No architectural accuracy requirements.

ID	Technical Requirement	Acceptance Criteria	ESS.	Satisfies	Verification Means
n/a	n/a	n/a	n/a	n/a	n/a

9.3 Extensibility

No extensibility requirements.

ID	Technical Requirement	Acceptance Criteria	ESS.	Satisfies	Verification Means
n/a	n/a	n/a	n/a	n/a	n/a

9.4 Configurability

The NAV3i Operating System offers the possibility to be configured for the different platforms of the NAV3i Platform Family during installation. The requirements are defined in the [DS_OS].
No further architectural requirements exist.

ID	Technical Requirement	Acceptance Criteria	ESS.	Satisfies	Verification Means
n/a	n/a	n/a	n/a	n/a	n/a

9.5 Maintainability

No further architectural maintainability requirements except those already listed in [DI_NAV3], [DI_NAV3I], [DI_NAVSUITE3] and [DS_OS].

ID	Technical Requirement	Acceptance Criteria	ESS.	Satisfies	Verification Means
n/a	n/a	n/a	n/a	n/a	n/a

9.6 Testability

No architectural testability requirements.

ID	Technical Requirement	Acceptance Criteria	ESS.	Satisfies	Verification Means
n/a	n/a	n/a	n/a	n/a	n/a

9.7 Persistency

No architectural persistency requirements.

ID	Technical Requirement	Acceptance Criteria	ESS.	Satisfies	Verification Means
n/a	n/a	n/a	n/a	n/a	n/a

9.8 Security

No further architectural security requirements except those already listed in [DI_NAV3], [DI_NAV3I], [DI_NAVSUITE3] and [DS_OS].

ID	Technical Requirement	Acceptance Criteria	ESS.	Satisfies	Verification Means
n/a	n/a	n/a	n/a	n/a	n/a

9.9 Performance

No further architectural performance requirements except those already listed in [DI_NAV3], [DI_NAV3I], [DI_NAVSUITE3] and [DS_OS].

ID	Technical Requirement	Acceptance Criteria	ESS.	Satisfies	Verification Means
n/a	n/a	n/a	n/a	n/a	n/a

9.10 Scalability

No architectural scalability requirements.

ID	Technical Requirement	Acceptance Criteria	ESS.	Satisfies	Verification Means
n/a	n/a	n/a	n/a	n/a	n/a

9.11 Reliability

No further architectural reliability requirements except those already listed in [DI_NAV3], [DI_NAV3I], [DI_NAVSUITE3] and [DS_OS].

ID	Technical Requirement	Acceptance Criteria	ESS.	Satisfies	Verification Means
n/a	n/a	n/a	n/a	n/a	n/a

9.12 Usability

No further architectural usability requirements except those already listed in in [DI_NAV3], [DI_NAV3I], [DI_NAVSUITE3] and [DS_OS].

ID	Technical Requirement	Acceptance Criteria	ESS.	Satisfies	Verification Means
n/a	n/a	n/a	n/a	n/a	n/a

9.13 Workflow Control

Workflows are implemented on application level. Each Navigation Application implements its own specific medical workflow.

ID	Technical Requirement	Acceptance Criteria	ESS.	Satisfies	Verification Means
n/a	n/a	n/a	n/a	n/a	n/a

9.14 Error Handling and Recovery

The NAV3i Operating System logs information about process crashes in error reporting files using the “Windows Error Reporting” service.. Additional error handling is provided by the Navigation Applications, like automatic restart and recovery after a crash.

No architectural error handling requirements exist except those already listed in in [DI_NAV3], [DI_NAV3I], [DI_NAVSUITE3] and [DS_OS].

ID	Technical Requirement	Acceptance Criteria	ESS.	Satisfies	Verification Means
n/a	n/a	n/a	n/a	n/a	n/a

9.15 Logging and Tracing

The NAV3i Operating System logs information on a low level basis (e.g. hardware errors or errors on process level) using the Windows event system. Additional logging is done by the Navigation Applications on high level, like logging of internal states and workflow transitions.

ID	Technical Requirement	Acceptance Criteria	ESS.	Satisfies	Verification Means
n/a	n/a	n/a	n/a	n/a	n/a

9.16 Parallelization and Threading

No architectural parallelization and threading requirements.

ID	Technical Requirement	Acceptance Criteria	ESS.	Satisfies	Verification Means
n/a	n/a	n/a	n/a	n/a	n/a

9.17 Internationalization

No further architectural internationalization requirements except those already listed in [DI_NAV3], [DI_NAV3I], [DI_NAVSUITE3] and [DS_OS].

ID	Technical Requirement	Acceptance Criteria	ESS.	Satisfies	Verification Means
n/a	n/a	n/a	n/a	n/a	n/a

9.18 Communication between Distributed Components

No architectural requirements.

ID	Technical Requirement	Acceptance Criteria	ESS.	Satisfies	Verification Means
n/a	n/a	n/a	n/a	n/a	n/a

9.19 Migration

No architectural requirements.

ID	Technical Requirement	Acceptance Criteria	ESS.	Satisfies	Verification Means
n/a	n/a	n/a	n/a	n/a	n/a

9.20 Configuration Management

No architectural requirements.

ID	Technical Requirement	Acceptance Criteria	ESS.	Satisfies	Verification Means
n/a	n/a	n/a	n/a	n/a	n/a

10 Design Decisions

This chapter lists all major design decisions which are considered noteworthy.

10.1 Operating System

The base operating system is Windows 8.1 Embedded Industry Pro (64bit).

Pros: State-of-the art operating system which supports all new hardware

Cons: All current applications need to be tested / adapted for Windows 8.1

10.2 One operating system for all platforms

All platforms of the NAV3i Platform Family share a common implementation of NAV3i Operating System.

Pros: Only one development effort for all platforms with reduced risk for issues on a single platform implementation

Cons: Higher complexity of implementation and installation

10.3 Frozen Software Versions

To protect the validated system configuration and to prevent Navigation Applications from malfunctioning, all parts of the NAV3i Operating System are configured in a way such that automatic updates are prevented when the system is connected to the Internet.

Pros: Validated system configuration is retained; applications always work as validated by system test.

Cons: Beneficial operating system patches get not installed in short time frame after release.

11 Development Environment

The final NAV3i Operating System is a compilation of the different software components (chapter 3.2) following the build procedure [BP_OS]. Finally the NAV3i Operating System image is built using the “Deployment Image Servicing and Management tool” which is part of [SW3].

Review Minute

Review Reference	**SOP 30-000 Software Development Plan** **The review team confirms, that the document meets the following requirements:** In case the system includes software: • the architecture of the software implements system and software requirements including those relating to risk control architecture; • the software architecture is able to support interfaces between software items and between software items and hardware; • the medical device architecture supports proper operation of any SOUP items; • the software safety classification has been re-evaluated.
Optional References	
Summary / Result	☐ **Review to be continued** ☐ **Accepted** (no further review) ☐ like it is ☐ minor changes (see list of findings) ☐ **Not accepted** (further review necessary) ☐ major changes (see list of findings) ☐ new revised version necessary
Follow Up	☐ **Execution and closure of all action items will be approved on document approval.** ☐ **Execution and closure of action items are deferred to the issue tracking system.** Issue(s): ☐ **Update of additional tangibles required** ☐ update of risk analysis required (add issue) Issue: ☐ update of other specification required (add issue): Issue:

Review Team

Name	Role

List of Findings

#	Ref. (Ref. No. / part)	Action Item	Resp.
1			

Signatures for document: System Architectural Design Description OS

Document Number: D0000039008NAV
Date: 2021-01-16 14:37:26.0
Revision: E
ECR Number:
ECN Number:

This document has been signed using an electronic signature within Windchill. To access the original source document and relevant information, please access the system directly.

Approval Information				
Group	Approval Role	Name	Date	Vote
	ARCHITECT	Becher Jochen	Mar 29, 2016 11:36:13 GMT	Approve
	PROJECTLEADER	Schoebel Alexander	Mar 29, 2016 07:00:53 GMT	Approve
	Author	Schoebel Alexander	Mar 29, 2016 07:00:39 GMT	Approve